LOCKING DOWN WINDOWS

COLLABORATING WITH NIST, NSA, AND DISA

Kurt Dillard – US Public Sector
kurt.dillard@microsoft.com

Don Armstrong – Government Security Program
Worldwide Public Sector

donalda@microsoft.com

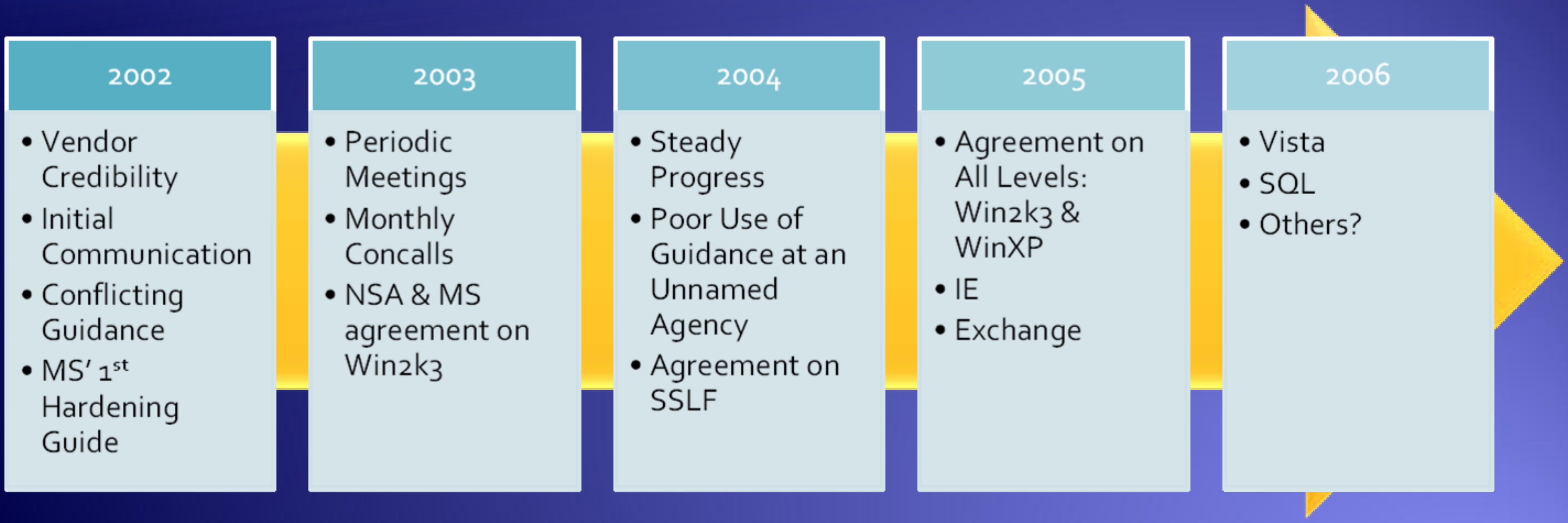
Agenda

- Some History
  - Windows 2000, Windows XP, Windows Server 2003 – Multiple Security Guides from multiple agencies.
  - Four years of progress
- Today
  - Vista and Longhorn security guidance
- Future
  - Continuing Commitment
  - XCCDF and OVAL formatted security configuration settings
  - Other Products

Why?

- Problem:
  - Lots of places to go for security guidance.
  - Conflicting security advice.
  - Applying the guidance often broke systems. E.g. PTO
    - http://support.microsoft.com/?id=823659 (focuse on MS guidance)
    - http://support.microsoft.com/?kbid=885409 (focus on 3rd party guides)
  - The value of some recommendations is difficult to understand and explain.
- Solution:
  - Get vendors & agencies to collaborate on recommended prescriptive security configurations and settings that are supported.
  - Balance increased security with functionality.
  - Ensure that vendors support configurations.

Timeline…



2002

- Vendor Credibility
- Initial Communication
- Conflicting Guidance
- MS’ 1st Hardening Guide

2003

- Periodic Meetings
- Monthly Concalls
- NSA & MS agreement on Win2k3

2004

- Steady Progress
- Poor Use of Guidance at an Unnamed Agency
- Agreement on SSLF

2005

- Agreement on All Levels: Win2k3 & WinXP
- IE
- Exchange

2006

- Vista
- SQL
- Others?

Key Accomplishments

- Introduced to the NSA late 2002.
- Worked closely with the NSA on Win2k3 high security settings – now SSLF settings.
- NSA endorsed our Win2k3 guide in August, 2003 by referencing Microsoft security guidance on NSA Web site.
- Agreement between NIST, DISA, NSA, and Microsoft in 2004 - 2005 on Win2k3 & WinXP.
- Recognition of the importance of this effort by Microsoft executives and security teams.
- Collaboration on Windows Vista guidance initiated months before it ships.
- Collaboration and co-development with numerous National and International Security and Intelligence agencies.

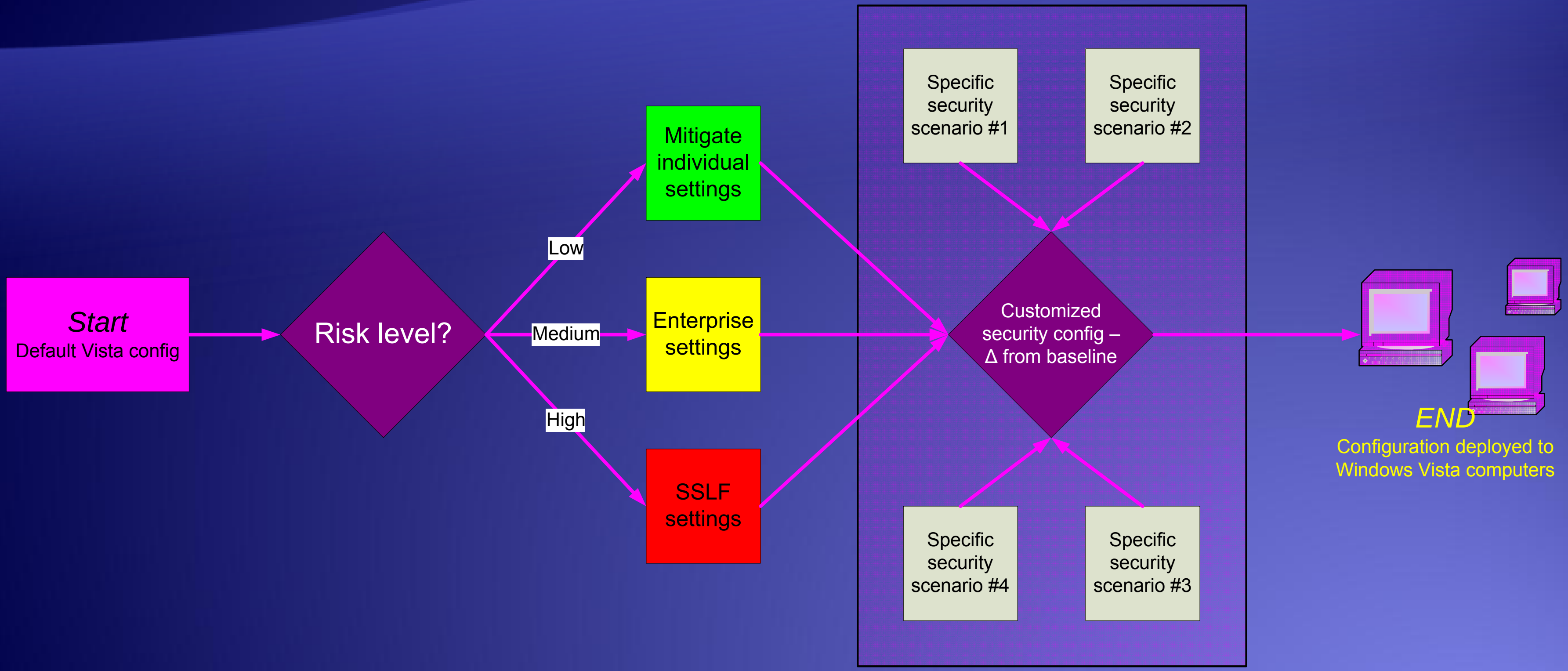
Now

- Don owns the global program from a corporate perspective through the Government Security Program.
- Microsoft Solutions for Security and Compliance owns creation & support of guidance for MS.
- Kurt is the strategic liaison focused on US.
- NSA & USAF have taken a lead on Vista settings.
- MSSC has developed the Vista Security Guide – now in Beta and available at. https://connect.microsoft.com/InvitationUse.aspx?ProgramID=820&InvitationID

The Windows Vista Security Guide

- Expansion from previous guides
  - Environment-based
  - Provides a variety of security levels
  - Business needs reflected in content
  - Includes scenario-based prescriptive security guidance
  - Includes AD configuration tool that reduces time to deployment in minutes instead of hours!
  - Configuration information ready for XCCDF and OVAL conversion.
- Leverages new Vista security technologies
  - BitLocker, User Account Control, etc.
  - Expanded GPMC configuration control
  - Use-as-appropriate based approach
- Note: Vista Security Guide is now in Beta!!
  - All specifications subject to change

How the VSG Works



Start
Default Vista config

Risk level?

Low

Medium

High

Mitigate individual settings

Enterprise settings

SSLF settings

Specific security scenario #1

Specific security scenario #2

Customized security config – Δ from baseline

Specific security scenario #4

Specific security scenario #3

END
Configuration deployed to Windows Vista computers

Scenarios

- Environments
  - Enterprise
  - Specialized Security Limited Functionality
- Specific mitigations
  - Defend Against Malware
  - Protect Sensitive Data
    - EFS, BitLocker, Smartcards
  - Consolidated Specialized Security Configuration
    - The sum of all countermeasures
  - Integrate and Support Legacy Applications
    - Compatibility features such as registry/file virtualization
    - UAC

Looking Ahead

- Vista guidance will be published simultaneously with Vista OS release
- Prescriptive Security Guidance for more products
  - Threats and Countermeasures guide for Vista
  - ISA 2006
  - Longhorn
  - Systems Center?
  - SQL Server
  - Exchange
  - Office 2007
- Expanding co-development efforts worldwide
- NIST Checklist approved and XCCDF / OVAL formatted security settings.

Links

- Windows Server 2003 Security Guide: http://go.microsoft.com/fwlink/?LinkId=14845
- Windows XP Security Guide: http://go.microsoft.com/fwlink/?LinkId=14839
- Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP: http://go.microsoft.com/fwlink/?LinkId=15159
- Windows 2000 Server Solution for Security: http://go.microsoft.com/fwlink/?LinkId=14837